



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-------------------------------------|-------------|----------------------|---------------------|------------------|
| 10/711,495 | 09/21/2004 | Terry M. Olkin | 60468.300901 | 5494 |
| 74029 | 7590 | 11/09/2007 | EXAMINER | |
| Patent Venture Group | | | CHAI, LONGBIT | |
| 10788 Civic Center Drive, Suite 215 | | | ART UNIT | PAPER NUMBER |
| Rancho Cucamonga, CA 91730-3805 | | | 2131 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 11/09/2007 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | |
|------------------------------|------------------------|---------------------|
| Office Action Summary | Application No. | Applicant(s) |
| | 10/711,495 | OLKIN ET AL. |
| | Examiner | Art Unit |
| | Longbit Chai | 2131 |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 11 October 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-26 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-26 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 21 September 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

1. At present, the pending claims are 1 – 26.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.
3. As per claim 1, Applicant asserts "Le Berre does not teach or reasonably suggest anything about hyperlinks having human and machine interpretable elements (Remarks: Page 3 / Last Para)". Examiner respectfully disagrees because Applicant's argument has no merit since the alleged limitation has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
4. In addition, As per claim 1, Applicant asserts (i) Applicant's "encrypted data" is tied to its "originator identifier", which is not just any encrypted data (e.g., its is not Le Berre's crypto-signature) (Remarks: Page 4 / Line 26 – 28) and (ii) One of ordinary skill in the art will appreciate that claim 1 employs decryption and that hashed data cannot be substituted for Applicant's "encrypted data" (Remarks: Page 5 / 26 – 28) and (iii) "hashed data cannot be substituted for encrypted data" (Remarks: Page 5 / 26 – 28). Examiner respectfully disagrees because Examiner notes the broadest and reasonable claim interpretations are made, according to MPEP 2111, such that (a) either a hashed value or a message can be considered as one type of computer data entities (b) the submitted rejection is not interpreting the hashed data as encrypted data and instead the submitted rejection broadly interprets that signing the hashed value by using a private key is broadly considered as an "encrypted data" to meet the

claim language since a data element encrypted, at the originate server A, using its private key is qualified as an "encrypted data" (Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 10 Line 31 – 32, Column 12 Line 56 – Column 13 Line 1 – 5 and Column 3 Line 42 – 45).

5. In addition, As per claim 1, Applicant asserts "Schneider in view of Le Berre does not teach presenting information on a display unit (Remarks: 6 / Line 15 – 17)". Examiner respectfully disagrees because Applicant's argument has no merit since the alleged limitation regarding what kind of particular information intended to be displayed has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. In addition, As per claim 1, Applicant asserts does not teach "presenting a confirmation of authentication to the user (Remarks: Page 6 / Line 25 – 27)". Examiner respectfully disagrees because Le Berre teaches successfully authenticating the signed URL and return the response to the user's browser (Le Berre: Column 8 Line 48-51) and as such Applicant's arguments are respectfully traversed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 3, 4, 6 – 9, 11 – 13, 15 – 18, 20, 21 and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Berre (Patent Number: EP 0940960 A1) in view of Schneider (U.S. Patent 6,760,746).

As per claim 1, Le Berre teaches a **computer program for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed** (Le Berre: Abstract, the last sentence and Column 5 Line 56 – 58), comprising:

a code segment that listens with a computerized system for an activation of the hyperlink (Le Berre: Column 7 Line 28 – 27 and Column 5 Line 56 – 58: an activation of the URL link);

a code segment that extracts an originator identifier and encrypted data from the hyperlink (Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 10 Line 31 – 32, Column 12 Line 56 – Column 13 Line 1 – 5 and Column 3 Line 42 – 45: (a) the originating server ID is qualified as an originator identifier and (b) a data element is encrypted at the originate server A by using its private key and (c) the receiving server B decrypts the data and checks the received signature from within the qualified set of servers. Therefore, the broadest and reasonable claim interpretations are made, according to MPEP 2111, such that a data element encrypted, at the originate server A, using its private key is qualified as an “encrypted data”);

a code segment that decrypts said encrypted data into decrypted data based on said originator identifier (Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 12 Line 51 – 52 and Column 12 Line 56 – Column 13 Line 1 – 5: (a) a data element is encrypted at the originate server A by using its private key (b) the receiving server B knows the corresponding public key of the originate server A and (c) the receiving server B decrypts the data and checks the received signature);

a code segment that redirects (Le Berre: Column 2 Line 30 – 34 and Column 6 Line 5 – 11; HTTP re-direction from server A to server B); and

a code segment that determines whether the hyperlink includes said originator identifier and said encrypted data decrypts successfully (Le Berre: Column 3 Line 42 – 45, Figure 5 and Column 6 Line 31 – 55 and Column 10 Line 31 – 32: the receiving server B decrypts the data and checks the received signature from within the qualified set of servers), and then:

runs said code segment that redirects, to redirect the user to the target URL (Le Berre: Figure 4 & Column 2 Line 30 – 34 and Column 6 Line 5 – 11);

Le Berre does not disclose expressly a code segment that presents information on a display unit; runs said code segment that presents, to present a confirmation of authentication to the user conveying the name of the owner and the domain name of the target URL, and otherwise, runs said code segment that presents, to present a warning dialog to the user.

Schneider in view of Le Berre teaches **a code segment that presents information on a display unit** (Schneider: Column 29 Line 9 – 13); **runs said code segment that presents, to present a confirmation of authentication to the user** (Le Berre: Column 8 Line 48 – 51: Le Berre teaches successfully authenticating the signed URL and return the response to the user's browser) **conveying the name of an owner and the domain name of the target URL** (Schneider: Column 29 Line 9 – 13: (a) displaying the URL information with the chosen target domain name being used as a re-direct URL and (b) the OriginateServerID as shown on the URL (Le Berre: Figure 5) that holds the private / public key is qualified as the name of the owner), **and otherwise, runs said code segment that presents, to present a warning dialog to the user** (Schneider: Column 12 Line 50 – 52 and Column 21 Line 52 – 53: an error

message upon the detection of an invalid URL (or not accessible) or with invalid domain name is displayed).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider within the system of Le Berre because (a) Le Berre teaches using a signed URI (Universal Resource Identifier) link to access a resource from the internet and to re-direct the client request from server A to another server B under the same network domain after authentication (Le Berre: Figure 4 & Column 2 Line 30 – 34 / Line 44 – 45 and Column 6 Line 5 – 11), and (b) Schneider discloses an enhanced presentation for clarity purpose by displaying the URL information with the chosen target domain name being used as a re-direct URL and also display an error message upon the detection of an invalid URL (or not accessible) or with invalid domain name (Schneider: Column 29 Line 9 – 13, Column 5 Line 56 – 58 and Column 3 Line 42 – 45).

As per claim 11 and 20, Le Berre teaches a system for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed (Le Berre: Abstract, the last sentence and Column 5 Line 56 – 58), the system comprising:

a logic in said computerized system that listens for activation of the hyperlink (Le Berre: Column 7 Line 28 – 27 and Column 5 Line 56 – 58: an activation of the URL link);

a logic that extracts an originator identifier and encrypted data from the hyperlink (Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 10 Line 31 – 32, Column 12 Line 56 – Column 13 Line 1 – 5 and Column 3 Line 42 – 45: (a) the originating server ID is qualified as an originator identifier and (b) a data element is encrypted at the originate server A by using its private key and (c) the receiving server B decrypts the data and checks the received signature from within the qualified set of servers);

a logic that decrypts said encrypted data into decrypted data based on said originator identifier ((Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 12 Line 51 – 52 and Column 12 Line 56 – Column 13 Line 1 – 5: (a) a data element is encrypted at the originate server A by using its private key (b) the receiving server B knows the corresponding public key of the originate server A and (c) the receiving server B decrypts the data and checks the received signature);

a code segment that redirects ((Le Berre: Column 2 Line 30 – 34 and Column 6 Line 5 – 11; HTTP re-direction from server A to server B);

a logic that determines whether the hyperlink includes said originator identifier and that said encrypted data decrypts successfully (Le Berre: Column 3 Line 42 – 45, Figure 5 and Column 6 Line 31 – 55 and Column 10 Line 31 – 32: the receiving server B decrypts the data and checks the received signature from within the qualified set of servers);

a logic responsive to said logic that determines, that redirects the user to the target URL (Le Berre: Figure 4 & Column 2 Line 30 – 34 and Column 6 Line 5 – 11); and

Le Berre does not disclose expressly a computerized system having a display unit; a logic responsive to said logic that determines, that presents on said display unit a confirmation of authentication conveying the name of the owner and the domain name of the target URL; and a logic responsive to said logic that determines, that presents on said display unit a warning dialog to the user.

Schneider in view of Le Berre teaches a computerized system having a display unit (Schneider: Column 29 Line 9 – 13); a logic responsive to said logic that determines, that presents on said display unit a confirmation of authentication (Le Berre: Column 8 Line 48 – 51) conveying the name of the owner and the domain name of the target URL (Schneider: Column 29 Line 9 – 13: (a) displaying the URL information with the chosen target domain name being

used as a re-direct URL and (b) the OriginateServerID as shown on the URL (Le Berre: Figure 5) that holds the private / public key is qualified as the name of the owner), and a logic responsive to said logic that determines, that presents on said display unit a warning dialog to the user (Schneider: Column 12 Line 50 – 52 and Column 21 Line 52 – 53: an error message upon the detection of an invalid URL (or not accessible) or with invalid domain name is displayed).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider within the system of Le Berre because (a) Le Berre teaches using a signed URI (Universal Resource Identifier) link to access a resource from the internet and to re-direct the client request from server A to another server B under the same network domain after authentication (Le Berre: Figure 4 & Column 2 Line 30 – 34 / Line 44 – 45 and Column 6 Line 5 – 11), and (b) Schneider discloses an enhanced presentation for clarity purpose by displaying the URL information with the chosen target domain name being used as a re-direct URL and also display an error message upon the detection of an invalid URL (or not accessible) or with invalid domain name (Schneider: Column 29 Line 9 – 13, Column 5 Line 56 – 58 and Column 3 Line 42 – 45).

As per claim 3, 12 and 21, Le Berre as modified teaches said code segment that listens runs as a service in said computerized system (Le Berre: Column 5 Line 24 – 27: running as a HTTP server to provide the authentication services).

As per claim 4 and 13, Le Berre as modified teaches said code segment that listens includes a hypertext transport protocol (HTTP) server (Le Berre: Column 5 Line 24 – 27: running as a HTTP server to provide the authentication services).

As per claim 6, 15 and 23, Le Berre as modified teaches said code segment that decrypts includes a code segment that extracts the target URL from said decrypted data (Le Berre: Column 6 Line 5 – 18).

As per claim 7, 16 and 24, Le Berre as modified teaches a code segment that extracts a digital signature from said decrypted data; and a code segment that verifies said digital signature against said originator identifier (Le Berre: Figure 5 and Column 6 Line 31 – 55, Column 12 Line 51 – 52 and Column 12 Line 56 – Column 13 Line 1 – 5: (a) a data element is encrypted at the originate server A by using its private key (b) the receiving server B knows the corresponding public key of the originate server A and (c) the receiving server B decrypts the data and checks the extracted signature).

As per claim 8 and 17, Le Berre as modified teaches said code segment that decrypts employs a public key associated with said originator identifier (Le Berre: Column 12 Line 56 – Column 13 Line 1 – 5 and Column 3 Line 42 – 45: (a) a data element is encrypted at the originate server A by using its private key (b) the receiving server B knows the corresponding public key of the originate server A and (c) the receiving server B decrypts the data and checks the received signature).

As per claim 9, 18 and 25, Le Berre as modified teaches a code segment that matches said originator identifier to one of a plurality of registered originators; and a code segment that retrieves a decryption key associated with said originator identifier for use by said code segment that decrypts (Le Berre: Column 3 Line 42 – 45 and Column 12 Line 56 – Column 13 Line 1 – 5: the receiving server B decrypts the data and checks the received signature from within the

qualified set of servers – i.e. by using the public key from within the qualified set of a plurality of originate servers).

2. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Le Berre (Patent Number: EP 0940960 A1) in view of Schneider (U.S. Patent 6,760,746), and in view of Dunnion et al. (U.S. Patent 2002/0199119).

As per claim 2, Le Berre as modified does not disclose expressly the computer program is digitally signed.

Dunnion teaches the computer program is digitally signed (Dunnion: Para [0099]: the entire downloaded program can be digitally signed for security reason to ensure that the software downloaded is actually that provided by the supplier and has not been replaced or altered).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Dunnion within the system of Le Berre as modified because (a) Le Berre teaches using a signed URI (Universal Resource Identifier) link to access a resource from the internet and to authenticate the requesting user with a signed data signature from within the qualified set of servers (Le Berre: Column 5 Line 56 – 58 and Column 3 Line 42 – 45), and (b) Dunnion teaches providing a method of a security services system where not only the data files and email traffic need to be secured but also the entire downloaded program can be digitally signed for security reason to ensure that the software downloaded is actually that provided by the supplier and has not been replaced or altered (Dunnion: Para [0005] and Para [0099]).

Art Unit: 2131

3. Claims 5, 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Berre (Patent Number: EP 0940960 A1) in view of Schneider (U.S. Patent 6,760,746), and in view of Perry (U.S. Patent 2003/0154306).

As per claim 5, 14 and 22, Le Berre as modified does not disclose expressly said code segment that listens at a preset non-routable internet protocol (IP) address and at a preset port.

Perry teaches said code segment that listens at a preset non-routable internet protocol (IP) address and at a preset port (Perry: Para [0025] Last sentence and Para [0024]: using a non-routable private IP address with a dynamically established port).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Perry within the system of Le Berre as modified because (a) Le Berre teaches using a signed URI (Universal Resource Identifier) link to access a resource anywhere from the internet and to re-direct the client request from server A to another server B under the same network domain (Le Berre: Figure 4 & Column 2 Line 30 – 34 / Line 44 – 45 and Column 6 Line 5 – 11), and (b) Perry teaches providing a non-routable private IP address with a dynamically established port for inbound connections with the advantage of conserving IP address, which are becoming increasingly difficult to acquire due to exhaustion of the limited IP address space (Perry: Para [0016] Last sentence and Para [0025] Last sentence).

4. Claims 10, 19 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Berre (Patent Number: EP 0940960 A1) in view of Schneider (U.S. Patent 6,760,746), and in view of Haitsuka et al. (U.S. Patent 6,766,369).

As per claim 10, 19 and 26, Le Berre as modified does not disclose expressly said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

Haitsuka teaches said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window (Haitsuka: Column 7 Line 35 – 37, Column 8 Line 44 – 47 and Column 10 Line 49 – 52: the display can have not only a browser window but also a client window; where the client window is generated / controlled by the local client application).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Haitsuka within the system of Le Berre as modified because (a) Le Berre teaches using a signed URI (Universal Resource Identifier) link to access a resource from internet by using a secured SSL (Session Security Layer) for the exchanges between the user and the server (Le Berre: Column 11 Line 8 – 10), and (b) Haitsuka teaches providing a flexible mechanism with a display having not only a browser window but also a client window; where the client window is generated / controlled by the local client application during a SSL communication session to indicate the connection status (including the authentication for a typical SSL connection) for the clarity purpose to avoid being confused with the display of browser window (Connery: Column 7 Line 35 – 37 and Column 10 Line 49 – 52 / Line 43 – 45).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


LBC

Longbit Chai
Examiner
Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100